

### ABSTRACT OF THE INVENTION

The present invention provides a method and apparatus for a trusted service provider (TSP) which assists with the secure exchange of data across the public switched telephone network. Communications are routed via a TSP, which uses cryptographic techniques to conceal the identities (e.g., telephone numbers) of the call initiator and call recipient, thereby preventing traffic analysis attacks. The TSP also performs cryptographic handshakes with the call initiator and call recipient to authenticate callers. The TSP further provides cryptographic keying material which communicants may use to help protect communications and to directly authenticate and identify each other. Although the TSP is trusted to negotiate the connection and is involved in the process, the communicants can perform their own key agreement and authentication for protecting data routed via the TSP.